The Apple/FBI case and the debates on the Snoopers’ Charter were among the most prominent developments this month, which brought privacy, security, and encryption in focus. Updates related to the EU-US Privacy Shield, which will replace the Safe Harbour agreement, are also on the Digital Policy Observatory’s radar for March.

The ‘IG building under construction’ illustration is symbolic of the ever-changing world of digital policy. A new iteration sees new elements that denote emerging trends, in addition to the existing robust foundation of IG topics. The illustration represents the taxonomy behind the GIP Digital Watch observatory.

The 31st session of the Human Rights Council saw important debates related to the digital world. Among them were privacy discussions in relation to the first report of the Special Rapporteur on the Right to Privacy - which includes a ten-point action plan aimed at increasing awareness and fostering cross-sectoral dialogue - and a discussion on online child sexual abuse.

The latest developments in the Apple/FBI case seem to bring the case to a close. But in reality, have the main dilemmas been resolved or are they likely to resurface in the near future? In another development, ICANN55 ended on a more positive note...

More on page 8

The IANA stewardship transition proposal and the ICANN accountability proposal were submitted to the US Government at the end of the week-long ICANN55th meeting, held in Marrakech, Morocco. We take a look at both proposals, and what the next steps are.

More on page 6

The IG building under construction illustration is symbolic of the ever-changing world of digital policy. A new iteration sees new elements that denote emerging trends, in addition to the existing robust foundation of IG topics. The illustration represents the taxonomy behind the GIP Digital Watch observatory.

More on page 2

In addition to this newsletter you can find in-depth coverage on the GIP Digital Watch observatory (http://digitalwatch.giplatform.org) and join live discussions on the last Tuesday of every month online, at local hubs, or at the Geneva Internet Platform premises | Geneva Digital Watch newsletter is published by the Geneva Internet Platform and DiploFoundation | Design by Viktor Mijatovic, Diplo’s CreativeLab | Authors of this issue: Stephanie Borg Psaila, Laetitia Honsberger, Aye Mya Nyein, Tereza Horejsova, Jovan Kurbalija, Virginia Paque, Roxana Radu, Vladimir Radunovic, Barbara Rosen Jacobson, Sorina Teleanu | Send your comments to digitalwatch@diplomacy.edu. A Brazilian version in Portuguese is available at http://giplatform.org/newsletter
On 9 March 2016, the Special Rapporteur on the Right to Privacy (SRP), Mr Joseph Cannataci, presented his first report at the 31st session of the Human Rights Council. Following the establishment of the SRP’s mandate in Resolution 28/18 (The right to privacy in the digital age), Cannataci took office in August 2015 and dedicated the first six months of his three-year mandate to consultations with stakeholders around the world. His report was positively received; the immediate diplomatic reactions stressed the importance of the role of privacy in flows of information in society; (b) rights taken in conjunction rather than in opposition (privacy and security rather than privacy vs security); (c) privacy as an enabling right rather than as an end in itself. The report draws on current developments around encryption, invalidation of the Safe Harbour agreement, and mass surveillance concerns to put forward its key theme: developing safeguards without borders and remedies across borders. It calls for cooperation across sectors to achieve the right to privacy and to ensure that various concerns and perspectives are taken into account.

In addition to seven in-depth thematic studies, the working methods adopted by the SRP and his team include country monitoring (based on a database of policies, laws, practices to map concerns and best-practices), review of individual complaints, joint actions, and public engagement activities. The SRP proposes a ten-point action plan meant to increase awareness and foster cross-sectoral dialogue, while preparing input for updating legal instruments through an expanded understanding of the right to privacy. The challenge, he concluded, is to provide a clear comprehensive vision and strong foundations which can form the basis of solid, evidence-based policy-making in the field of privacy protection.

The Special Rapporteur’s ten-point action plan aims to facilitate the process of further elaboration on the dimensions of the right to privacy and its relationship with other human rights:

1. Going beyond the existing legal framework to a deeper understanding of what it is that we have pledged to protect
2. Increasing awareness of privacy among citizens
3. Creating a structured, on-going dialogue about privacy
4. Adopting a comprehensive approach to legal, procedural and operational safeguards and remedies
5. Placing a renewed emphasis on technical safeguards
6. Engaging in a specially-focused dialogue with the corporate world
7. Promoting national and regional developments in privacy-protection mechanisms
8. Harnessing the energy and influence of civil society
9. Clarifying key concepts such as cyberspace, cyber-privacy, cyber-espionage, cyberwar and cyberpeace through thematic studies
10. Investing further in international law

Anytime you see this icon, there is more background material in the digital version. Alternatively, visit www.giplatform.org/digitalwatch for more in-depth information.
EDITORIAL: OF PRIVACY, SECURITY, AND THE IANA TRANSITION

The Apple/FBI case, which pretty much dominated the discussions on privacy, security, and encryption in March, took a surprising U-turn when the FBI announced it may have found a way to unlock the phone without Apple’s assistance. The confirmation came on 28 March; the government said it was now able to do so with the assistance of an undisclosed third party.

The case brought several dilemmas to the forefront, which we summarised in a series of blog posts played out by three fictitious characters, representing the security, privacy, and commercial sides of the debate.

The latest developments seem to bring the case to a close, with the US government asking the court to vacate the order. But in reality, have the main dilemmas been resolved or are they likely to resurface in the near future? In addition, we are faced with new concerns: if a third party has managed to unlock the phone, is it only a matter of time before the software’s vulnerabilities are exploited? Who will get to them first?

While we were closely following the Apple/FBI developments, the community involved in the IANA stewardship transition process was busy finalising the transition and ICANN accountability proposals in Marrakech (read more on page 6). The good news is that they were both submitted to the US government at the end of ICANN’s 55th public meeting. They will now undergo independent reviews, which we will follow over the next few months.

All in all, the first quarter of 2016 was a busy time for digital policy. We started the year as techno-realists, and were immediately drawn into discussing the emerging business model and its related challenges. These developments bring into sharper focus the need to develop new models of consensus, or an Internet social contract (read more on page 7).

APPLE/FBI CASE: DEVELOPMENTS IN MARCH

The Apple/FBI case, which became a global controversy in the past few weeks, took a turn when the FBI announced it may have found a way to unlock the phone without Apple’s assistance. On 28 March, the US government confirmed it was now able to do so with the assistance of a third party. The government also asked the court to vacate its order compelling Apple to assist the FBI.

The Apple/FBI controversy started soon after a California District Court confirmed an order requesting Apple to assist the FBI in unlocking the iPhone of a terrorist responsible for killing 14 people in San Bernardino. Apple’s strong opposition to the order gained the support of other major tech companies.

A string of developments took place in the past few weeks. Among the developments was a ruling over a drug case by a New York District Court, in which the magistrate ruled that the US Department of Justice cannot force Apple to provide the FBI with access to a locked phone - a ruling which the Justice Department has sought to overturn.

The following is a timeline of the main developments, surrounding the Apple/FBI case, which took place in March.

1 Mar: Apple and the FBI testify before the Judiciary Committee in the US Congress.
2 Mar: In a letter to the court, the UN Special Rapporteur for Freedom of Expression, David Kaye, states that the FBI risks violating the International Covenant on Civil and Political Rights.
4 Mar: Apple receives support from several companies, including Microsoft, Amazon, Google, Facebook, Yahoo!, and Cisco (in one brief), and Twitter, LinkedIn, eBay, and Airbnb (in another brief).
4 Mar: The UN High Commissioner for Human Rights, Zeid Ra’ad Al Hussein, issues a statement, stating that the ramifications of the case go beyond the issue at hand and ‘could have extremely damaging implications for the human rights of many millions of people, including their physical and financial security’.
8 Mar: The US Department of Justice seeks to overturn a New York judge’s drug case ruling.
On 29 February, the judge ruled that the Justice Department cannot force Apple to assist the FBI in unlocking an iPhone, in a case unrelated to the San Bernardino case.
10 Mar: In a new court filing, the Justice Department argues that the FBI’s request does not represent an ‘undue burden’ for the company, and that the order is limited to a specific case.
16 Mar: Apple’s reply argues that it cannot comply with the court’s order, as this would go against the US Constitution.
22 Mar: The US government asks the court to cancel the anticipated 22 March hearing as the FBI may have found a way to unlock the iPhone without Apple’s assistance.
28 Mar: The US government drops its case against Apple; the Justice Department announces that it is now able to unlock the iPhone with the assistance of a third party.
New appointments were made in relation to the IGF’s Multistakeholder Advisory Group (MAG), tasked to provide advice on IGF preparations. The UN Secretary-General appointed Lynn St Amour (USA) as chair; the members of the renewed MAG were also announced.

The UN has issued a call for stakeholder contributions on key issues related to achieving the sustainable development goals (SDGs). The contributions will feed into the High-level Thematic Debate on achieving the SDGs, in New York next month.

Preparations for the first multistakeholder forum on science, technology, and innovation, taking place in New York in June, are under way. The 10-member group to support the Technology Facilitation Mechanism (10-MG) for achieving the SDGs have identified the objectives and theme, and have tackled other preparations leading up to the forum.

The OSCE’s 57 participating states have agreed to expand the organisation’s list of confidence-building measures (CBMs). Among other measures, states will ‘encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information’, on a voluntary basis. The new measures build on the first round of CBMs adopted in 2013.

The Apple/FBI case dominated the discussions on security, privacy, and encryption this month. The debate turned global, while testimonies of the main players continued. In a surprising U-turn, the US government announced that it is was able to unlock the iPhone with the assistance of a third party (Read more on page3).

Similar debates on privacy and surveillance took place in the UK parliament over the Investigatory Powers Bill, dubbed the Snooper’s Charter, which remains controversial due to its data retention requirements.

The Special Rapporteur on the Right to Privacy, Joseph Cannataci, presented the first report of his mandate at the 31st session of the Human Rights Council; developing safeguards without borders and remedies across borders is a key theme of the report, which proposes a ten-point action plan.

The French data protection regulator (Commission nationale de l’informatique et des libertés - CNIL) has fined Google €100,000 for failing to extend its delisting of search results across all of Google’s domain name extensions.

The Article 29 Working Party is currently reviewing the legal texts issued by the European Commission that will put in place the EU-US Privacy Shield.

New VoIP services are now blocked in Morocco, further fuelling the controversy over banned VoIP services. Telecom providers have declared that the decision to ban VoIP calls, in place since January, was taken by the regulator.

Google is currently in talks with Indian telecom operators to kickstart the Loon project in India. The project uses balloons instead of land-based infrastructure to provide Internet access to rural areas. Google gained support from the Indian government early this year.

This year’s Global Encryption Trends Study reports that companies storing sensitive data in the cloud are increasingly encrypting such data.
Net neutrality
FCC rules put to the test: T-mobile adds more services to its Binge On service, which allows users to stream content that is not counted towards their data cap. Verizon, AT&T, and Comcast offer similar packages.

After the zero-rating ruling, the Indian Telecom Regulatory Authority (TRAI) will finalise a comprehensive review of net neutrality within the next few months, following a request by the country’s Department of Telecommunications.

E-commerce and Internet economy
The UK’s latest budget provides for tax relief for micro-entrepreneurs who sell their services online or rent their homes through the Internet. India is looking into expanding the so-called Google Tax through an ‘equalising levy’ of 6-8% on gross payment ‘if the provider of the service is a foreign entity without a “permanent establishment” in India’.

The European Commission’s first findings of a sector inquiry on e-commerce reveal the widespread use of geo-blocking in Europe, while guidelines on how to apply existing EU legislation to the ‘sharing economy’ are expected to be published in June 2016.

Jurisdiction and legal issues
Six of the largest tech companies have criticised the Snoopers’ Charter, as it attempts to establish extra-territorial jurisdiction, allowing the country to force companies to comply even if they are not based in the UK.

In a preliminary opinion, the Advocate General (AG) of the European Court of Justice has declared that operators of free public WiFi should not be held accountable for copyright infringements committed by users of their networks. If the Court confirms the AG’s opinion, Germany could be forced to change its law that holds WiFi providers responsible for illegal activity.

IANA Transition
The ICANN Board submitted the plan to transition stewardship of key Internet functions to the US government. The plan includes both the IANA stewardship transition proposal and the supplemental final proposal on ICANN accountability recommendations. The US government announced that it has contracted the Berkman Center at Harvard University to perform an independent review of the proposals by 30 June.
This month has been a turning point for the IANA transition process, as the IANA stewardship transition proposal and the ICANN accountability proposal were submitted to the US government. The submissions came at the end of the week-long ICANN 55th public meeting, held in Marrakech, Morocco, 5-10 March.

Proposed changes to IANA stewardship

The IANA stewardship transition proposal, finalised in October 2015, contains three distinct proposals, from the three communities directly affected by the transition: the domain names community, the numbering resources community (mainly the Internet Regional Registries responsible for the regional allocation and management of IP addresses), and the protocol parameters community (represented by the Internet Engineering Task Force (IETF) and the Internet Architecture Board).

While the numbers and protocol parameters communities generally proposed the maintenance of their current relationships with ICANN as the IANA functions operator, with some review mechanisms in place, the domain names community’s proposal outlines several significant changes. It envisions the creation of a separate legal entity (Post Transition IANA), as a subsidiary of ICANN, which would become the IANA functions operator (IFO) for the domain names, on the basis of a contract with ICANN. Therefore, IANA functions would continue to be performed within the ICANN framework, but a clearer separation between the technical functions and the policy-making functions of ICANN would be established. There are also provisions in the proposal underlying the conditions under which a review process could lead to a separation of the IFO from ICANN. Major changes in the DNS root zone, currently subject to formal approval by the US government, would be authorised by the ICANN Board of Directors.

Proposed changes to ICANN’s accountability

The accountability proposal outlines a series of recommendations aimed to make ICANN more accountable to the global Internet community. The main recommendation concerns the creation of a new legal entity (the ‘empowered community’) that would function as an unincorporated association and would be able to enforce a set of community powers, such as removing members of the ICANN Board, rejecting ICANN budgets, or rejecting changes to the ICANN bylaws. This entity would act as instructed by the ‘decisional participants’ - most of ICANN’s constituencies. In order to ensure a more active and consistent engagement of the community in ICANN’s decision-making processes, the proposal introduces an obligation for the Board to engage in an extensive engagement process with the community before making major decisions on issues such as strategic and operating plans, modifications to ICANN bylaws, or reviews of the IANA functions. If the community is not satisfied with the results of such processes, it could exercise one of its powers. As a last resort mechanism, if the community decides to remove Board members or recall the entire Board, but the Board refuses to comply with such a decision, a claim could be brought in a court that has jurisdiction to force compliance with the decision.

Status of the two proposals and next steps

Work on the accountability proposal was finalised in Marrakech. While most of ICANN’s constituencies approved the proposal, the Governmental Advisory Committee (GAC) only said that it did not object to the proposal being sent to the ICANN Board. This was because of concerns raised by several governments with regard to certain parts of the proposal, which were seen as undermining GAC’s role within ICANN (more details here).

On 10 March, the ICANN Board received the IANA stewardship transition and the ICANN accountability proposals, and submitted them to the US government, which announced its intention to review the proposals within 90 days, as well as its expectation that, before the review is completed, ICANN would adopt the bylaw changes that are required for the implementation of the proposals. US Congress, which already held a hearing on the IANA stewardship transition on 17 March, will most probably also perform its own review of the proposals.

More details about the IANA transition process can be found on a dedicated page at the GIP Digital Watch observatory.
The dilemmas arising from the Apple/FBI case, which converged around privacy, security, users’ trust, and business models, were among the most debated topics in March, and for good reason. The courts were faced with one of the most pressing issues of modern politics: how to safeguard both privacy and security, and if not possible, how to strike the right balance between the two.

Given the prominence of the case, the issues were also the subject of a series of blog posts, published on DiploFoundation’s website in March, which attempted to recreate a Socratic dialogue between three fictitious characters, representing the security, privacy, and commercial sides of the debate.

The conversations show that although the Apple/FBI crisis is resolved, no solution for similar cases that may emerge in the future has yet been found. All major actors in this debate have legitimate interests, vulnerabilities, and limited power. Users, governments, or the business sector could not impose their will in this case, but the combination of legitimate interests and limited power among all stakeholders could be a starting point for compromise and, ultimately, a new social contract.

What also underlines this discussion is the growing distrust in democratic institutions. It is worth debating how the security community can rebuild the trust of citizens, such as by taking wise decisions on encryption, rather than encouraging situations where citizens place their trust in commercial entities without any democratic control, or are left to take their own security measures.

It is reasonable to believe that a due process mechanism can be put in place, and that clear and reasonable conditions and limitations can be set for cases in which authorities ask tech companies for assistance in bypassing security measures built for devices. Users also need guarantees.

Given that the US political system is based on political checks-and-balances, any emerging arrangement could be based on ‘multistakeholder’ checks-and-balances, involving the government, users, and businesses. These could be the first building blocks of an Internet social contract.
The ‘IG building under construction’ illustration is symbolic of the ever-changing world of digital policy. Developed by Diplo-Foundation, the concept was first brought to life in 2004. The building had five storeys, which represented the five ‘baskets’ or categories of the IG debate: infrastructure and standardisation, legal, economic, development, and sociocultural.

An updated version in 2014 saw two new storeys added to the building: cybersecurity and human rights. The seven floors, or baskets, became the taxonomy behind the GIP Digital Watch observatory, a neutral one-stop shop dedicated to IG issues, incorporating live developments, overviews and explanatory texts, events, resources, and other content related to Internet governance and digital policy. Meanwhile, the illustration has received another iteration.

The latest version of the IG building is now more robust. The floors and elements in each section of the building are clearly defined. Pillars, elevators, and machinery transport several crucial components across the storeys. A cloud appears for the first time. Other elements, representing new trends, help further define the building. It is representative of the state of play of IG today: we are on our way, but not quite there yet. Will the building be completed soon?

View all the iterations of the ‘IG building under construction’